

RECEIVED

Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, D.C. 20554

MAY 20 1998

FEDERAL COMMUNICATIONS COMMISSION
OFFICE OF THE SECRETARY

In the Matter of

Communications Assistance for Law Enforcement
Act

CC Docket No. 97-213

COMMENTS OF SBC COMMUNICATIONS INC.

JAMES D. ELLIS
ROBERT M. LYNCH
DURWARD D. DUPRE
LUCILLE M. MATES
FRANK C. MAGILL

175 E. Houston, Room 4-H-40
San Antonio, Texas 78205
(210) 351-5575

ROBERT VITANZA

15660 Dallas Parkway, Suite 1300
Dallas, Texas 75248
(972) 866-5380

Its Attorneys.

Date: May 19, 1998

No. of Copies rec'd
List A B C D E

022

SUMMARY

With respect to the scope of the assistance capability requirements of CALEA, carriers are truly “caught in the middle”, facing multiple statutory mandates that appear at some points to be contradictory, particularly in light of CALEA’s legislative history and the positions already taken by other interested parties in this proceeding.

The law enforcement community, as represented by the FBI/DOJ Petition for Expedited Rulemaking (“the FBI/DOJ Petition”), asserts that CALEA requires inclusion in the “safe harbor” industry standard, J-STD-25, of a number of enhanced surveillance capabilities that were considered and rejected by the TR45.2 Subcommittee as being beyond the scope of CALEA. Privacy advocates, represented by the Center for Democracy and Technology Petition for Rulemaking (“CDT Petition”), take the opposite view and assert that J-STD-25 already goes too far in providing law enforcement with surveillance capabilities in excess of those intended by Congress.

For the reasons set forth herein, SBC respectfully submits that the Commission should resolve the current dispute over J-STD-25 by finding that, in its present form, it constitutes a “safe harbor” pursuant to Section 107 of CALEA, 47 U.S.C. §1006, and further by acting in the manner suggested in the April 9, 1998 joint filing of the CTIA, the Personal Communications Industry Association (PCIA) and the United States Telephone Association (USTA).

The interim industry standard balances the competing interests of law enforcement, privacy and industry innovation in a manner consistent with the intent of congress, and should be approved as a “safe harbor” under 47 U.S.C. §1006(a).

The enhanced capabilities sought by the FBI/DOJ petition are beyond the intended scope of CALEA. SBC respectfully suggests that the FBI/DOJ must bear the burden of persuading the

Commission that their extremely broad interpretation of CALEA's assistance capability requirements should be adopted. As indicated by the following discussion, as well as by the several petitions and responses already filed by industry groups before the FCC in this proceeding, law enforcement stands alone among all the interested parties, and on extremely shaky legal ground at that, in arguing that the "punch list" capabilities are required by CALEA. Unfortunately, the FBI/DOJ petition fails to provide any sound arguments in support of the "punch list". Instead, as before, the FBI/DOJ present a series of conclusory legal assertions unsupported by relevant case law or traditional means of statutory interpretation.

Congress quite clearly did not intend for CALEA to require that law enforcement be afforded every possible enhancement to its electronic surveillance capabilities simply because such an enhancement may be technologically possible and would benefit a particular investigation. What Congress did intend was to balance the interests of law enforcement against those of the protection of privacy and the fostering of innovation in the telecommunications network. Each of the enhanced surveillance capabilities on the "punch list" represents a sharp departure from these principles of CALEA interpretation.

CDT overstates the significance of the two items in J-STD-25 which are the subjects of its contention that the industry already has agreed to features that exceed the permissible scope of CALEA-compliant capabilities. CALEA does not prohibit all efforts to derive location information based on wireless intercepts. Contrary to CDT's contention, delivery of call content and call identifying information together in the packet switching environment, and relying on law enforcement to obey the law by not intercepting content if not authorized properly to do so, is not a change from the *status quo*.

In light of the intent of Congress regarding CALEA implementation, *i.e.* that the industry is in the best position to determine the method and manner of CALEA compliance, and given the showing above that establishes the sufficiency of J-STD-25 as a “safe harbor” standard under the law, the FCC should remand the standard to the Subcommittee with directions to produce a final standard with such adjustments as the FCC finds necessary and appropriate as a result of this proceeding. J-STD-25 deserves to become the governing standard for CALEA compliance because it carefully balances the policy interests advanced by Congress in its framing of the statute, contrary to the gold-plated wish list represented by the FBI’s ESI document and the proposed rule attached to the FBI/DOJ petition to which these Comments respond. While this wish list might indeed advance the laudable interests of more effective law enforcement, such were not the only interests deemed important by Congress. Most importantly, the FCC must act quickly. If law enforcement feels that the provisions of CALEA do not adequately meet its needs, then its remedy lies on Capitol Hill, rather than before this Commission.

Table of Contents

I. <u>INTRODUCTION</u>	1
II. <u>THE INTERIM INDUSTRY STANDARD BALANCES THE COMPETING INTERESTS OF LAW ENFORCEMENT, PRIVACY AND INDUSTRY INNOVATION IN A MANNER CONSISTENT WITH THE INTENT OF CONGRESS, AND SHOULD BE APPROVED AS A “SAFE HARBOR” UNDER 47 U.S.C. §1006(a)</u>	4
<u>A. The Enhanced Capabilities Sought By The FBI/DOJ Petition Are Beyond The Intended Scope Of CALEA.</u>	6
<u>B. The Portions of J-STD-25 Criticized By The CDT Petition Do Not Exceed The Requirements of CALEA.</u>	15
III. <u>THE PENDING CTIA PETITION FOR RULEMAKING SHOULD BE CONSIDERED FULLY BY THE COMMISSION, ALONG WITH THE OTHER INDUSTRY ASSOCIATION PETITIONS REFERRED TO IN THE PUBLIC NOTICE.</u>	16
IV. <u>THE TR45.2 SUBCOMMITTEE IS BEST SUITED TO PRODUCE A FINAL CALEA COMPLIANCE STANDARD INCORPORATING THE FCC’S FINDINGS IN THIS PROCEEDING.</u>	16
V. <u>THE RELIEF REQUESTED IN THE JOINT RESPONSE OF USTA, CTIA AND PCIA TO THE FBI/DOJ PETITION SHOULD BE GRANTED.</u>	17
VI. <u>CONCLUSION</u>	17

Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, D.C. 20554

In the Matter of

Communications Assistance for Law Enforcement
Act

CC Docket No. 97-213

COMMENTS OF SBC COMMUNICATIONS INC.

I. INTRODUCTION

SBC Communications Inc., on behalf of its affiliates Southwestern Bell Telephone Company, Pacific Bell, Nevada Bell, Southwestern Bell Wireless Inc., Southwestern Bell Mobile Systems, Inc., and Pacific Bell Mobile Services, Inc. (collectively "SBC"), responds to the Commission's Public Notice¹ inviting comments on the scope of the assistance capability requirements of the Communications Assistance for Law Enforcement Act ("CALEA"), 47 U.S.C. §1001 *et seq.*, on the various pending Petitions raising issues concerning the sufficiency, or lack thereof, under CALEA of the existing interim standard known as J-STD-25 (TIA Subcommittee TR45.2),² and on the joint motion of the Federal Bureau of Investigation/Department of Justice (FBI/DOJ) to dismiss the July 16, 1997 Petition for Rulemaking filed by the Cellular Telecommunications Industry Association ("the CTIA Petition").

¹ Communications Assistance for Law Enforcement Act, *Public Notice*, CC Docket No. 97-213, DA 98-762, rel. April 20, 1998.

² *Id.*, at pp. 3-4.

With respect to the scope of the assistance capability requirements of CALEA, carriers are truly “caught in the middle”, facing multiple statutory mandates that appear at some points to be contradictory, particularly in light of CALEA’s legislative history and the positions already taken by other interested parties in this proceeding. On the one hand, carriers are required by pre-existing Federal wiretapping law³, as well as by CALEA, to render technical assistance to law enforcement in the carrying out of electronic surveillance. CALEA further requires carriers to facilitate law enforcement’s access to call identifying information, and to enable law enforcement to intercept wire and electronic communications, all pursuant to court order or other lawful authorization.

On the other hand, CALEA requires carriers to provide the foregoing to law enforcement in a manner that minimizes interference with subscribers’ service, and protects the privacy of communications not authorized to be intercepted. In addition, carriers face potential civil liability to aggrieved persons, under Federal civil rights and wiretapping laws⁴, should they participate in or enable unlawful or unconstitutional electronic surveillance, if their actions are later found by a court or jury to have been unreasonable.⁵

As the legislative history makes abundantly clear, Congress sought in enacting CALEA “to balance three key policies: (1) to preserve a narrowly focused capability for law enforcement agencies to carry out properly authorized intercepts; (2) to protect privacy in the face of increasingly powerful and personally revealing technologies; and

³ 18 U.S.C. §2518(4).

⁴ 42 U.S.C. §1983; 18 U.S.C. §2520.

⁵ Although acting in good faith reliance on a court order or other lawful authorization is a complete defense to an action under either of the statutes cited in Note 4, *supra*, that defense only applies if the carrier’s subjective good-faith belief in the lawfulness of its actions is found to have been reasonable under all the circumstances. See *Jacobson v. Rose*, 592 F2d 515 (9th Cir. 1978), *cert den* 442 US 930 (1979).

(3) to avoid impeding the development of new communications services and technologies.”⁶ Not surprisingly, various interested parties apply differing interpretations to the appropriate weight due each of these competing policy considerations. The law enforcement community, as represented by the FBI/DOJ Petition for Expedited Rulemaking (“the FBI/DOJ Petition”), asserts that CALEA requires inclusion in the “safe harbor” industry standard, J-STD-25, of a number of enhanced surveillance capabilities that were considered and rejected by the TR45.2 Subcommittee as being beyond the scope of CALEA. Privacy advocates, represented by the Center for Democracy and Technology Petition for Rulemaking (“CDT Petition”), take the opposite view and assert that J-STD-25 already goes too far in providing law enforcement with surveillance capabilities in excess of those intended by Congress.

Thus, as noted previously, carriers are caught in the crossfire between these polar opposites, resulting in derogation of the third policy objective of CALEA, that of not impeding the development of new communications services and technologies. The standards process has been disrupted and then placed under a cloud of uncertainty by the actions and arguments of law enforcement and privacy advocates. As a result, the industry is unable to meet the statutory compliance date of October, 1998, and is reluctant to roll out new technologies and services absent some clear idea of the validity of the “safe harbor” standard, as well as the extent to which the potentially huge development and manufacturing costs of CALEA-mandated retrofitting and compliance will be reimbursed by the Federal government.

⁶ House Report 103-827 and Senate Report 103-402, at p. 13. Because these Reports are nearly identical, future citations will be made only to the House Report.

For the reasons set forth below, SBC respectfully submits that the Commission should resolve the current dispute over J-STD-25 by finding that, in its present form, it constitutes a “safe harbor” pursuant to Section 107 of CALEA, 47 U.S.C. §1006, and further by acting in the manner suggested in the April 9, 1998 joint filing of the CTIA, the Personal Communications Industry Association (PCIA) and the United States Telephone Association (USTA), to wit:

- Determine that compliance with the CALEA assistance capability requirements is not reasonably achievable at this time using currently available technology;
- Remand to TIA Subcommittee TR45.2 any change in the industry standard brought about by this proceeding;
- Toll the CALEA compliance date during the rulemaking process;
- Grant an industry-wide extension of the compliance date for two years from the date of the Commission’s rule to allow sufficient time to implement the standard, with any revisions the Commission finds necessary and proper; and
- Ensure that any rule the FCC issues is voluntary, to preserve carriers’ choice as to how CALEA’s assistance capability requirements should be implemented.⁷

II. THE INTERIM INDUSTRY STANDARD BALANCES THE COMPETING INTERESTS OF LAW ENFORCEMENT, PRIVACY AND INDUSTRY INNOVATION IN A MANNER CONSISTENT WITH THE INTENT OF CONGRESS, AND SHOULD BE APPROVED AS A “SAFE HARBOR” UNDER 47 U.S.C. §1006(a).

The interim industry standard, J-STD-25, was adopted after approximately two years of monthly meetings and even more frequent consultations among representatives of carriers, manufacturers and of various law enforcement agencies (LEAs), principally the FBI.⁸ The format of an interim standard was rendered necessary only because, contrary to the spirit of cooperative consultation intended by Congress, the FBI and other LEAs blocked the approval of the first standard for the very reason now at issue in this proceeding, *i.e.*, the proposal (SP-3580) did not contain the enhanced surveillance

⁷ *Public Notice*, DA 98-762, at p. 4, note 6.

⁸ SBC concurs with and hereby incorporates by reference the sequence of events involved in the standard-setting process as set forth in Section I, Background, of the CTIA Petition.

capabilities now sought by the FBI/DOJ Petition.⁹ These capabilities have become known as the “punch list”, and will be referred to as such in these Comments from time to time.

The interim standard represents a carefully crafted, good-faith compromise between the desires of LEAs for a perfect, all-encompassing system for electronic surveillance and the strong concerns of carriers and other industry parties that the true intent of CALEA be preserved, as well as carriers’ additional concerns that exceeding such intent could expose them to undue risk of civil liability in litigation brought by “aggrieved parties” under 18 U.S.C. §2520 and/or under 42 U.S.C. §1983. Contrary to the assertions contained in the CDT Petition, the standard-setting process has at no time been conducted “behind closed doors”,¹⁰ but has been open to contributions from interested parties, as is customary for standards set under ANSI auspices. Indeed, CDT itself contributed its comments to the TR45.2 Subcommittee,¹¹ and of course the present proceeding is open to public comment.

As explained more fully below, SBC continues to support J-STD-25 as the only reasonable path to timely CALEA implementation consistent with the clearly expressed

⁹ Congress expressed its intent regarding the process of CALEA implementation in relevant part as follows: “[47 U.S.C. 1006] establishes a mechanism for implementation of the capability requirements that defers, in the first instance, to industry standards organizations. Subsection (a) directs the Attorney General and other law enforcement agencies to consult with associations and standard-setting bodies of the telecommunications industry. Carriers, manufacturers and support service providers will have a “safe harbor” and be considered in compliance with the capability requirements if they comply with publicly available technical requirements or standards designed in good faith to implement the assistance requirements.... Subsection (b) provides a forum at the Federal Communications Commission in the event a dispute arises over the technical requirements or standards.” House Report 103-827, Part I, pp. 26-27. SBC suggests that, rather than prolonging the process and endangering industry’s ability to meet the original CALEA compliance date by blocking approval of SP-3580 in the spring of 1997, the FBI and other LEAs should instead have brought the issue promptly before the Commission, as they now have done, and as Congress clearly intended.

¹⁰ CDT Petition at p. 6.

¹¹ *Id.*, at p. 4.

intent of Congress. The positions of both the FBI/DOJ Petition and the CDT Petition should be rejected because they are extreme interpretations that fail to reflect the balancing of interests envisioned by CALEA's framers.

A. The Enhanced Capabilities Sought By The FBI/DOJ Petition Are Beyond The Intended Scope Of CALEA.

SBC respectfully suggests that the FBI/DOJ must bear the burden of persuading the Commission that their extremely broad interpretation of CALEA's assistance capability requirements should be adopted. As indicated by the following discussion, as well as by the several petitions and responses already filed by industry groups before the FCC in this proceeding, law enforcement stands alone among all the interested parties, and on extremely shaky legal ground at that, in arguing that the "punch list" capabilities are required by CALEA.

Ever since the FBI first introduced its "wish list" for CALEA implementation in April of 1996, the so-called "Electronic Surveillance Interface" document ("ESI"), FBI representatives have maintained to SBC and other industry representatives that the ESI, and only the ESI or its functional equivalent, can constitute a "safe harbor" standard under 47 U.S.C. §1006(a). In other words, the consistent position of the FBI has been that every capability set forth in the ESI is required, and that any standard not containing each of those capabilities would be "deficient", under 47 U.S.C. §1006. Throughout the time since the ESI was first issued, the industry has insisted unanimously that certain surveillance capabilities specified therein (*i.e.* the "punch list") not only are not required by CALEA, but in fact are either well beyond CALEA's intended scope or are prohibited outright by the statutory language and its underlying legislative intent.

Also throughout the period since April, 1996, industry representatives have repeatedly requested that the FBI provide industry with the legal analysis that FBI representatives, in several meetings and discussions, asserted would support their position, and thereby allay the industry's concerns about potential liability exposure should the disputed capabilities be embedded in the national telecommunications network. No such analysis has ever been provided.

SBC welcomed the news early in 1998 that the FBI and DOJ were finally preparing to bring this dispute to the FCC, in part because it was hoped that the long-awaited analysis would finally appear; unfortunately, the FBI/DOJ petition fails to provide any sound arguments in support of the "punch list". Instead, as before, the FBI/DOJ present a series of conclusory legal assertions unsupported by relevant case law or traditional means of statutory interpretation. In some instances, the FBI/DOJ arguments are directly contrary to clear statements of Congressional intent contained in the House Report¹², and in several other points the FBI/DOJ petition simply makes outright misstatements of fact. Most frequently, however, the FBI/DOJ petition recites over and over again the same refrain that industry has heard since the first issue of the ESI document: the enhanced capabilities are technologically available, and critically important to law enforcement, in that their absence from the industry standard will deprive LEAs of important evidence. Therefore, says this argument, such capabilities must be required by CALEA.

¹² See, e.g., FBI/DOJ petition, paragraph 45, where it is contended that the assistance capability requirements are not restricted "to those communications and call-identifying information that were accessible to law enforcement in the pre-digital era." This contention flies in the face of the House Report, which states: "The FBI Director testified that the legislation was intended to preserve the status quo, *that it was intended to provide law enforcement no more and no less access to information than it had in the past.*" (Emphasis added.) House Report 103-827, at p. 22.

Neither SBC nor any other company in the industry would take issue with the assertion that many of the “punch list” capabilities would assist LEAs in obtaining useful evidence in criminal investigations. This, however, is not at all relevant to the issues now before the Commission. Congress quite clearly did not intend for CALEA to require that law enforcement be afforded every possible enhancement to its electronic surveillance capabilities simply because such an enhancement may be technologically possible and would benefit a particular investigation. What Congress did intend was, as stated previously herein, to balance the interests of law enforcement against those of the protection of privacy and the fostering of innovation in the telecommunications network.

In its Committee Reports on CALEA, Congress made the following statement concerning the intended interpretation of the law:

“The Committee intends the assistance requirements in section 2602 [now 47 U.S.C. §1002] to be both a floor and a ceiling. The FBI Director testified that the legislation was intended to preserve the status quo, that it was intended to provide law enforcement no more and no less access to information than it had in the past. The Committee urges against overbroad interpretation of the requirements. The legislation gives industry, in consultation with law enforcement and subject to review by the FCC, a key role in developing the technical requirements and standards that will allow implementation of the requirements. The Committee expects industry, law enforcement and the FCC to narrowly interpret the requirements.” House Report 103-827, at pp. 22-23.

Each of the enhanced surveillance capabilities on the “punch list” represents a sharp departure from these principles of CALEA interpretation.

1. Conference Calls Without “Target Party” On Line.

The FBI/DOJ petition goes to great length in attempting to convince the Commission that Title III (18 U.S.C. 2510, *et seq.*) permits a court-ordered intercept of any communications “supported by” a target subject’s equipment, facilities or services, regardless of whether or not the target party, *i.e.* the party named in the court order, is

actually on the line. Accordingly, FBI/DOJ maintain that CALEA §103 (47 U.S.C. §1002) requires carriers to provide the capability to monitor the conversations of parties to a three-way or conference call with a target after the target has dropped off the line or placed the other parties on hold, even though Paragraph 51 of the FBI/DOJ petition admits that failure to provide this capability “does not amount to a reduction in the information that has been available to law enforcement” prior to CALEA. This, of course, ignores the sworn testimony of FBI Director Freeh, as cited in the House Report¹³ and quoted above, that CALEA was not intended to provide law enforcement with any more access to information than it previously had. Interim standard J-STD-25 maintains the *status quo*, and as such is clearly sufficient.

2. Party Join, Party Hold, and Party Drop Messages.

Law enforcement contends, again without any real support other than its bald assertion of CALEA coverage and dire warnings of the potential loss of important evidence, that these types of messages constitute “call identifying information” as defined in 47 U.S.C. §1001, and therefore are mandated under §1002. If this language stood alone, without any relevant industry custom and usage and without relevant legislative history, then perhaps the FBI/DOJ would have a valid argument, at least with respect to party join/hold/drop messages that are fully available to a carrier in its own switch, and thus might be reasonably available to the carrier.¹⁴ The language does not stand alone,

¹³ Note 12, *supra*.

¹⁴ If a conference call bridge is external to the target subscriber carrier’s switch, (*i.e.* the conferencing service is provided by a different carrier, possibly outside the first carrier’s service area), a frequent occurrence in the modern environment, then provision of the capability to report such messages to law enforcement becomes a tremendous technical challenge that may or may not even be possible. Given the cost likely to be involved, such capability certainly is not reasonably available to the subscriber’s carrier. The FBI/DOJ petition makes no mention of the “reasonably available” requirement of 47 U.S.C. §1002(a)(2). In any event, the legislative history also makes clear that when a call is directed to another

however: both custom and usage in the industry and the statute's legislative history indicate that law enforcement's interpretation is invalid. "Call identifying information" means the signals, pulses or tones that *initially* set up and direct a call, not signals, etc. sent after a call is established. Moreover, as with the conference call capabilities discussed above, Paragraph 77 of the FBI/DOJ petition admits that party hold and party drop messages were not previously available to law enforcement officials conducting pen register intercepts. Thus, CALEA's legislative history clarifies that Congress did not intend to require that these messages be added to the long-standing industry definition of "call identifying information".¹⁵ The interim standard is therefore sufficient in this regard.

3. Subject-Initiated Dialing and Signaling.

This item of law enforcement's wish list involves the use of feature keys, flash hook presses, and dialing of digit keys for various purposes following initial establishment of the call ("cut-through"). (FBI/DOJ petition, paragraphs 61-72). Once again, as noted in 2., above, these signals do not fit the traditional concept of "call identifying information". Furthermore, to the extent that they have not previously been available through pen register intercepts, they constitute access to additional information that Congress expressly stated it did not intend to provide in CALEA. The FBI/DOJ's attempts to argue around these examples of Congressional intent either contradict this intent, or are of no relevance to the issue at hand. For example, in Footnote 17 at paragraph 67, the FBI/DOJ petition complains that certain post-cut-through dialing

carrier, the original carrier is responsible only for providing law enforcement with the identity of the other carrier, not for all information generated in the further progress of the call. House Report at p. 22.

¹⁵ House Report at p. 22; Note 12, supra.

information is now digitized, and asserts that such information is now not capable of being interpreted by law enforcement through use of a pen register. If that is the case, then the FBI/DOJ's citation (petition, footnote 20) of the New York Telephone case¹⁶ would seem to stand for the opposite proposition to that for which it is advanced by FBI/DOJ: given that information obtained from a pen register is not "call content", then anything *not* obtainable by use of a pen register is *call content that may be obtained only pursuant to a Title III order*.

Similarly, in its footnote 19, at paragraph 70, the FBI/DOJ petition takes the FCC's ruling in Docket No. 96-388¹⁷ entirely out of context. While a call may only be "completed" for purposes of pay telephone compensation and reclassification when the called party answers, for purposes of CALEA the same reasoning does not necessarily apply. This is particularly true where, as in the case of a call to an 800 calling card service, the information law enforcement seeks regarding the ultimate destination of the call may not even be available to the target subscriber's carrier. Thus, even if this information constitutes "call identifying information", which SBC denies, it is not "reasonably available" to the originating carrier as required by CALEA. (47 U.S.C. §1002(a)(2)).

4. Network-Generated In-Band or Out-of-Band Signaling.

In its paragraph 80, the FBI/DOJ petition takes to new heights its misconstruction of the language and intent of CALEA's definition of "call identifying information". Network-generated signals such as call waiting, ringing or busy signals have nothing to

¹⁶ United States v. New York Telephone Co., 434 U.S. 159 (1977) (dialing information obtained by a pen register device does not constitute call content requiring a Title III court order).

¹⁷ In re Implementation of the Pay Telephone Reclassification and Compensation Provisions of the Telecommunications Act of 1996 (Sept. 20, 1996).

do with origin, direction, destination or termination of a call, no matter how severely one twists their meaning. In addition, these tones cannot reasonably be detected from the network or the originating or terminating switches; thus, they are not reasonably available to carriers, even if they constitute “call identifying information”. In any event, to the extent that these signals can be audibly detected over the target subscriber’s line, they constitute *call content*, and can be obtained through a properly authorized Title III intercept. If they cannot be audibly detected, they are neither call content nor call identifying information, and are therefore not covered by CALEA.

5. Timing of Delivery of Call Identifying Information.

In another effort to divert attention from the real issue here, the FBI/DOJ petition (paragraphs 86-93) contains references to preventing murders, kidnappings and bombings, claiming that delivery of call identifying information to law enforcement within three seconds of an event and making time stamps accurate to within 100 milliseconds are both required by CALEA. Of course, in virtually the next breath, the petition all but admits that such is not the case. (See paragraphs 91, 93).

Despite these scare tactics, the FBI/DOJ petition can point to no actual case in which the timing of a carrier’s delivery of call identifying information has ever led to a crime that otherwise would have been prevented. More importantly, the fact is that the timing of delivery of call identifying information is a function of network and equipment design, and thus law enforcement is prohibited from dictating an arbitrary timing requirement by 47 U.S.C. §1002(b)(1). Law enforcement, the FCC and the public may, however, rest assured that carriers and manufacturers will put forth their best efforts to

provide call identifying information as rapidly and efficiently as possible, in full compliance with CALEA.

6. Surveillance Status Messages and Continuity Checks.

These features have nothing to do with call identifying information or the content of communications. They merely verify that an intercept is operational, a function that is adequately provided for in the interim standard. While CALEA requires that carriers ensure their capability of intercepting communications and isolating call identifying information, as the FBI/DOJ petition asserts at paragraph 94, CALEA does not require that carriers constantly confirm this to law enforcement in real time. Test procedures already are available by which law enforcement can perform this function in concert with carrier personnel. Again, the FBI/DOJ petition here seeks to dictate the manner in which the industry complies with CALEA, which Congress expressly intended to leave to carriers.¹⁸

7. Feature Status Message.

This demand by law enforcement relates to information that currently is provided pursuant to subpoena, indicating a subscriber's service profile. Apparently desiring to reduce its administrative work load and shift the burden to carriers, law enforcement here equates subscriber-initiated changes in features *that are not associated with any call* to "call identifying information", and demands that carriers provide such information in automated, real-time fashion. This does not even meet the grossly expanded definition of this term relied upon elsewhere in the FBI/DOJ petition. It amounts to nothing more than a convenience for law enforcement, and one that would impose large costs on carriers.

¹⁸ House Report at p. 19.

Furthermore, such a capability is not reasonably achievable, even through the use of subpoenas, in light of the implementation of many “per call” features offered through Advanced Intelligent Networks.

8. Dialed Digit Extraction/ Standardization of Delivery Interface Protocols.

With respect to these functions, law enforcement once again argues with the industry over the manner in which delivery of call identifying information will take place. Law enforcement urges the Commission to order that all digits dialed after a call is set up be delivered over a call data channel (CDC), rather than delivering some or all of the digits over a separate call content channel (CCC). In addition to violating the prohibition against law enforcement mandating the design or configuration of networks or services, this demand presumes that all such dialed digits are in fact “call identifying information”, which as shown in sections 2 and 3, above, is not the case. Accordingly, this item exceeds the scope of the CALEA assistance capability requirements. Finally, the FBI/DOJ petition argues at paragraph 84 that CALEA requires carriers to “employ the most efficient and effective means of delivering authorized surveillance information to law enforcement.” SBC is unable to find any such requirement specified in CALEA; indeed, as noted previously, ¹⁹ Congress intended that the determination of the methods of CALEA compliance be left to the industry.

Similar problems are inherent in law enforcement’s demand that a ceiling be placed on the number of interface protocols used by carriers to deliver content and call identifying information. The FBI/DOJ complain that this leaves carriers free to determine such protocols, entirely ignoring the fact that this is precisely the result that Congress intended.

B. The Portions of J-STD-25 Criticized By The CDT Petition Do Not Exceed The Requirements of CALEA.

CDT overstates the significance of the two items in J-STD-25 which are the subjects of its contention that the industry already has agreed to features which exceed the permissible scope of CALEA-compliant capabilities. CDT takes the position that the standard converts all wireless phones into location-tracing devices, which is not the case. All that is provided is the ability to identify the landline central office through which a roaming cellular call is routed. In any event, CALEA does not prohibit all efforts to derive location information based on wireless intercepts. It merely prohibits the derivation of location information from intercepts that are authorized solely under the provisions of the Federal statutes applicable to pen register or trap and trace devices.²⁰

CDT also accuses the industry of exceeding CALEA's scope on the issue of packet switched signals. Contrary to CDT's contention, delivery of call content and call identifying information together in the packet switching environment, and relying on law enforcement to obey the law by not intercepting content if not authorized properly to do so, is not a change from the *status quo*. That is exactly what happens now in many, if not most, pen register situations--a carrier opens a circuit to law enforcement attached to the subject's line, from which law enforcement frequently has the capability to listen to content in addition to the tones that are interpreted by a DNR (dialed number recorder) or other "pen register" device. It is not the function of a carrier to monitor law

¹⁹ Text accompanying note 18, *supra*.

²⁰ 47 U.S.C. §1002(a)(2)(B). Furthermore, the FCC itself already has ordered that, for purposes of emergency 911 systems, wireless carriers must install the capacity to pinpoint the location of a wireless 911 caller within the next three years. In the Matter of Revision of the Commission's Rules to Ensure Compatibility With Enhanced 911 Emergency Calling Systems, Docket No. 94-102, rel. 7/26/96.

enforcement's compliance with 18 U.S.C. §2510 *et seq.*--that job is properly left to the courts.

Additionally, although digital technology is capable of separating content from call-identifying information in the packet switching environment, it would be extremely difficult and costly, and therefore is not reasonably achievable.

III. THE PENDING CTIA PETITION FOR RULEMAKING SHOULD BE CONSIDERED FULLY BY THE COMMISSION, ALONG WITH THE OTHER INDUSTRY ASSOCIATION PETITIONS REFERRED TO IN THE PUBLIC NOTICE.

The FBI/DOJ Joint Motion to Dismiss CTIA's July, 1997 Petition for Rulemaking relies solely on the contention that the issuance of J-STD-25 renders the petition moot and unworthy of Commission consideration. SBC disagrees with this contention. So long as the current cloud of uncertainty generated by law enforcement's own Expedited Petition for Rulemaking remains in the CALEA sky, no party's views on the need for, or the proper contents of, a "safe harbor" industry standard should be ignored. CTIA certainly should not be penalized simply for being the first party to submit a filing on the issue, and as the representative of a major segment of the telecommunications industry, it is entitled to have its initial petition considered along with the views it has expressed in later filings.

IV. THE TR45.2 SUBCOMMITTEE IS BEST SUITED TO PRODUCE A FINAL CALEA COMPLIANCE STANDARD INCORPORATING THE FCC'S FINDINGS IN THIS PROCEEDING.

In light of the intent of Congress regarding CALEA implementation, *i.e.* that the industry is in the best position to determine the method and manner of CALEA compliance, and given the showing above that establishes the sufficiency of J-STD-25 as a "safe harbor" standard under the law, the FCC should remand the standard to the

Subcommittee with directions to produce a final standard with such adjustments as the FCC finds necessary and appropriate as a result of this proceeding. This would also serve the FCC's interests, in that it would avoid the assumption of a large burden that would amount, essentially, to "re-inventing the wheel." If necessary, the Commission can expedite its oversight role by providing that the final standard be submitted for FCC approval before becoming effective.

V. THE RELIEF REQUESTED IN THE JOINT RESPONSE OF USTA, CTIA AND PCIA TO THE FBI/DOJ PETITION SHOULD BE GRANTED.

SBC adopts and incorporates by reference herein the arguments advanced by these industry associations in their April 9, 1998 filing, in addition to the arguments set forth in SBC's own Petition for Extension of the CALEA compliance date.

VI. CONCLUSION.

SBC welcomes the Commission's effort to untangle the mess that CALEA compliance has become, and urges the Commission to give due consideration in its deliberations to the good faith effort that the industry has put forth over the past several years since the enactment of CALEA. J-STD-25 deserves to become the governing standard for CALEA compliance because it carefully balances the policy interests advanced by Congress in its framing of the statute, contrary to the gold-plated wish list represented by the FBI's ESI document and the proposed rule attached to the FBI/DOJ petition to which these Comments respond. While this wish list might indeed advance the laudable interests of more effective law enforcement, such were not the only interests deemed important by Congress. Most importantly, the FCC must act quickly, because the unnecessary controversy over the "punch list" generated by the law enforcement community, certainly with the best of intentions, has inexcusably ground the entire

process of CALEA compliance to a halt, and is interfering with the design and deployment of new communications technologies and services that the public wants and needs. It is time for the industry to get back to the business of providing these technologies and services. If law enforcement feels that the provisions of CALEA do not adequately meet its needs, then its remedy lies on Capitol Hill, rather than before this Commission.

Respectfully submitted,

SBC COMMUNICATIONS INC.



JAMES D. ELLIS
ROBERT M. LYNCH
DURWARD D. DUPRE
LUCILLE M. MATES
FRANK C. MAGILL

175 E. Houston, Room 4-H-40
San Antonio, Texas 78205
(210) 351-5575

ROBERT VITANZA

15660 Dallas Parkway, Suite 1300
Dallas, Texas 75248
(972) 866-5380

Its Attorneys.

Date: May 19, 1998

Certificate of Service


I, Mary Ann Morris, hereby certify that the foregoing, "Comments of SBC Communication Inc." in Docket No. 97-213 has been filed this 20th day of May, 1998 to the Parties of Record.


Mary Ann Morris

May 20, 1998

05/07/95 15:40 FAX 214 958 0287

FED. DKT. MGMT

 LARRY BERMAN
JAMES X. DEMPSEY
CENTER FOR DEMOCRACY AND TECHNOLOGY
1634 EYE STREET, N.W.
SUITE 1100
WASHINGTON, DC 20006

LARRY R. PARKINSON
GENERAL COUNSEL
FEDERAL BUREAU OF INVESTIGATION
935 PENNSYLVANIA AVENUE, N.W.
WASHINGTON, DC 20535

DOUGLAS N. LETTER
APPELLATE LITIGATION COUNSEL
CIVIL DIVISION
U.S. DEPARTMENT OF JUSTICE
601 D STREET, N.W., ROOM 9106
WASHINGTON, DC 20530

GRANT SEIFFERT
MATTHEW J. FLANIGAN
1201 PENNSYLVANIA AVENUE, N.W.
SUITE 315
WASHINGTON, DC 20004

ALBERT GIDARI
PERKINS COIE LLP
1201 THIRD AVENUE
40TH FLOOR
SEATTLE, WASHINGTON 98101

STEWART A. BAKER
THOMAS M. BARBA
JAMES M. TALENS
L. BENJAMIN EDERINGTON
STEPTOE & JOHNSON LLP
1330 CONNECTICUT AVENUE, N.W.
WASHINGTON, DC 20036

AT&T WIRELESS SERVICES, INC.
DOUGLAS I. BRANDON
1150 CONNECTICUT AVE.
4TH FLOOR
WASHINGTON, DC 20036

LUCENT TECHNOLOGIES INC.
DEAN L. GRAYSON
1825 EYE STREET, N.W.
WASHINGTON, DC 20006

ERICSSON INC.
CATHERINE WANG
SWIDLER & BERLIN
3000 "K" STREET, NW
SUITE 300
WASHINGTON, DC 20007